LA IMPORTANCIA DEL HACKING ÉTICO EN EL SECTOR FINANCIERO

Danilo Alberto Burgos Rivera
Universidad Piloto de Colombia
Bogotá, Colombia
daburgosriv@gmail.com

***Resumen*—** a través del siguiente artículo se hará una observación en cuanto la importancia de mantener periódicamente un análisis de vulnerabilidades que embarca el concepto de hacking ético en el sector financiero, ya que son las entidades con mayor número de ataques, son el mayor objetivo de los delincuentes, por esta razón el hacking ético es la medida que ayuda a cerrar los baches de seguridad los cuales son necesarios para mitigar los riesgos en este tipo de compañías.

***Abstract*—** Usually the companies that receive are hacking attempts that have to do with financial systems, since they are the ones responsible for managing financial transactions, personal information of clients, credit cards and keys, turns out to be tentative for evildoers attempt to violate and take economic advantage, which is why today the financial organizations are more dependent on technology than in previous years, the use of consumer services such as online payment services, purchases and transfers puts target favorite attackers. A need to implement ethical hacking is to facilitate hazard mitigation story vulnerabilities that are present at all times.

***Palabras claves* —** amenazas cibernéticas, confidencialidad disponibilidad, vulnerabilidades, hacker, hacking ético, hackers de sombrero blanco, hackers de sombrero negro, integridad.

I. INTRODUCCIÓN

En la actualidad, las empresas que más sufren de intentos de **hackeo** son las del sector financiero, lo anterior se debe a que estas entidades realizan actividades relacionadas con movimientos de dinero y por ende tienen el poder sobre la información de sus clientes (información personal y claves para realizar estas transacciones). Tal situación, termina tentando a los malhechores que intentan vulnerar los sistemas para sacar provecho económico.

Por tal razón, las organizaciones financieras en pro de cumplir con su función de salvaguardar los recursos captados del público y de diversificar su portafolio de servicios ha implementado el uso de herramientas de información, como ejemplo de esto son los servicios de: pagos en línea, compras y transferencias cuyo objetivo es ofrecer al cliente plataformas en línea seguras para evitar el traslado al banco. Sin embargo, para incentivar el uso de estas herramientas fue necesario la promulgación de la ley 527 de 1999 para otorgar confianza y seguridad a las relaciones que se den en internet, es así como las entidades financieras junto con la Superintendencia Financiera se ven comprometidas al uso de medidas de Hacking Ético para facilitar la mitigación de riesgos a través de la detección temprana de posibles vulnerabilidades que por lo general están presentes en todo momento.

Raytheon|Websense dio a conocer el Reporte 2015 *Financial Services Drill-Down* de *Websense Security Labs*, el cual examina el estado actual de las **amenazas cibernéticas** y de los ataques que buscan robar datos y que afectan a las instituciones de servicios financieros. Esta investigación revela un alto grado de especialización entre los criminales que atacan a los servicios financieros, una gran inversión en la fase de señuelo, y los ataques específicos y anómalos dirigidos a los objetivos globales en el sector financiero.[1]

El Reporte 2015 *Financial Services Drill-Down* muestra que los servicios financieros sufrieron incidentes de seguridad con 300 por ciento más frecuencia que otras industrias. Bajo un bombardeo constante de los criminales cibernéticos, el número

de ataques contra el sector financiero supera al volumen promedio de ataques contra otras industrias en una proporción de tres a uno. Además, la sofisticación y la persistencia de los ataques siguen planteando desafíos a los profesionales de la seguridad. [2]

Websense: Es una compañía de defensa estadounidense, especializada en software de seguridad informática. Esta empresa genera informes sobre las vulnerabilidades según el tipo de empresa, exponiendo así, cuales son los ataques más frecuentes.

II. HACKING ÉTICO

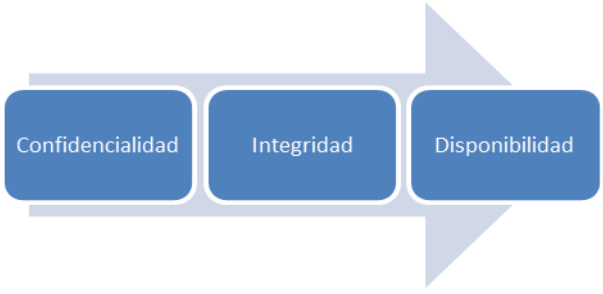
A. *Definición*

El hacking ético: Es en sí una auditoría efectuada por profesionales de seguridad de la información, quienes reciben el nombre de *"**pentester**"*. A la actividad que realizan se le conoce como "**hacking ético**" o "pruebas de penetración".

Las pruebas de penetración surgieron como respuesta a la presencia y realización de los primeros ataques informáticos a las organizaciones, los cuales trajeron graves consecuencias, como pérdidas monetarias y de reputación. Es aquí donde interviene el trabajo de un "**hacker ético**", ya que su labor es buscar vulnerabilidades en los sistemas de la organización para, posteriormente, poder mitigarlos y evitar fugas de información sensible. [3]

B. *Elementos de seguridad*

Figura 1- Elementos principales de seguridad que pueden ser vulnerados



Fuente: Elaboración propia

Confidencialidad: Evitar que la información pueda ser conocida o leída por personas no autorizadas.

1) **Disponibilidad:** Garantizar que la información y/o los componentes del sistema se encuentran accesibles en el momento en que una persona, proceso o aplicación los requiera.
2) **Integridad**: garantizar que la información no sea modificada.

C. *Tipos de hacker*

Las dos categorías principales en los hacker son los de sombrero blanco y sombrero negro.

1) Hackers de sombrero blanco (White Hat Hackers): se refiere a los expertos en seguridad informática que se especializan en realizar pruebas de penetración con el fin de asegurar que los sistemas de información y las redes de datos de las empresas. Estos hackers cuando encuentran una vulnerabilidad inmediatamente se comunican con el administrador de la red para comunicarle la situación con el objetivo de que sea resuelta lo más pronto posible.

2) Los hackers de sombrero negro (Black Hat Hackers): son los **hackers** que se infiltran en redes y computadoras con fines maliciosos. Los hackers de **sombrero negro** continúan superando tecnológicamente a los **sombreros blancos**. A menudo se las arreglan para encontrar el camino de menor resistencia, ya sea debido a un error humano o pereza, o con un nuevo tipo de ataque.[4]

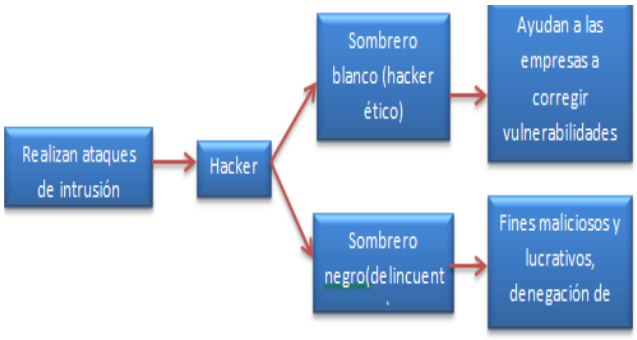
A diferencia de un hacker de **sombrero blanco**, el hacker de **sombrero negro** se aprovecha de las vulnerabilidades con el objetivo de destruir o robar información.

D. *Objetivos del hacking ético*

- Evaluar el estado de seguridad de un sistema o infraestructura tecnológica.
- Explotar las **vulnerabilidades** encontradas sin perjudicar la red ni los activos de la organización.

- Analizar los resultados obtenidos.
- Reportar a las partes interesadas.
- Dar las mejores recomendaciones para **mitigar el riesgo** de las vulnerabilidades que se encuentren.

Figura 2- Tipos de hacker que existen



Fuente: Elaboración propia.

III. NORMAS Y LEYES APLICABLES PARA HACKING ÉTICO

A. Circular 042 del 2012

En el numeral 7 se especifican los requerimientos para un análisis de **vulnerabilidades**, en esta se describen los requerimientos mínimos de seguridad y calidad para la realización de operaciones bancarias.

Esta ley indica los requisitos que las entidades financieras deben implementar en sus sistemas de análisis de vulnerabilidades, donde se destacan:

a) Estar basado en un **hardware de propósito específico** (appliance) totalmente separado e independiente de cualquier dispositivo de procesamiento de información, de comunicaciones y/o de seguridad informática.
b) Generar de manera automática por lo menos dos (2) veces al año un informe consolidado de las vulnerabilidades encontradas. Los informes de los últimos dos años deberán estar a disposición de la SFC.
c) Las entidades deberán tomar las medidas necesarias para mitigar las **vulnerabilidades** detectadas en sus análisis.
d) Realizar un análisis diferencial de **vulnerabilidades**, comparando el informe actual con respecto al inmediatamente anterior.
e) Las herramientas usadas en el análisis de **vulnerabilidades** deberán estar homologadas por el **CVE** (Common Vulnerabilities and Exposures) y actualizadas a la fecha de su utilización.
f) Para la generación de los informes solicitados se deberá tomar como referencia la lista de nombres de vulnerabilidades CVE publicada por la corporación Mitre (www.mitre.org).[5]

B. ISO 27001

Es una norma internacional que permite el aseguramiento, la **confidencialidad** e integridad de los datos y de la información, así como de los sistemas que la procesan.
El estándar ISO 27001:2013 para los **Sistemas Gestión de la Seguridad** de la Información permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.[6]

C. PCI DSS

Este estándar ha sido desarrollado por un comité conformado por las compañías de tarjetas (débito y crédito) más importantes, comité denominado PCI SSC (Payment Card Industry Security Standards Council) como una guía que ayude a las organizaciones que procesan, almacenan y/o transmiten datos de tarjetahabientes (o titulares de tarjeta), a asegurar dichos datos, con el fin de evitar los fraudes que involucran tarjetas de pago débito y crédito.

Las compañías que procesan, guardan o trasmiten datos de tarjetas deben cumplir con el estándar o arriesgan la pérdida de sus permisos para procesar las tarjetas de crédito y débito (Perdida de

franquicias), enfrentar auditorías rigurosas o pagos de multas1 Los Comerciantes y proveedores de servicios de tarjetas de crédito y débito, deben validar su cumplimiento al estándar en forma periódica. [7]

IV. NORMA QUE COMPROMETE A LAS ENTIDADES FINANCIERAS A DAR SEGURIDAD EN LA INFORMACIÓN DE LOS CLIENTES

A. Ley 1328 del 2009

Esta ley es medio de la cual se dictan algunas normas en materia financiera respecto a las obligaciones en las que se puede entender la importancia de la **confidencialidad** de la información la cual los clientes esperan sean mantenidas en secreto y que los datos que se suministran a estas entidades estará segura, esto se ve detalladamente en el artículo 7 el cual nombra las obligaciones especiales de este tipo de entidades, son dos ítems los cuales se aprecia el valor de la información personal.

Artículo 7. i) Guardar la reserva de la información suministrada por el consumidor financiero y que tenga carácter de reservada en los términos establecidos en las normas correspondientes, sin perjuicio de su suministro a las autoridades competentes.

Artículo 7. q) Disponer de los medios electrónicos y controles idóneos para brindar eficiente seguridad a las transacciones, a la información **confidencial** de los consumidores financieros y a las redes que la contengan. [8]

La información es **confidencial** y lo ideal es que no exista ingreso sin autorización a estos datos personales, ya que podría ser utilizada de forma inadecuada. Ejemplo de esto, se da con el robo de identidad, donde se suplanta a un usuario para realizar compras de bienes, contratar servicios de terceros, etc., (todo esto posible con los datos personales), lo anterior puede traer graves consecuencias para los usuarios y para la misma entidad financiera. Puesto que en algunos casos no solo se adquiere bienes y servicios sino que se llega a adquirir créditos de vivienda, con lo que no solo puede desembocar en deudas injustificables que traen como consecuencia ser reportados en la central de riesgos. Esto último, traería un impacto negativo en la vida crediticia del usuario y de la entidad financiero, ya que el usuario se vería afectado para adquirir nuevos créditos y la entidad se vería envuelta en investigaciones y en la perdida de la cartera prestada.

Es un riesgo real el cual siempre existirá, deberemos ser cuidadosos en las transacciones y tomar medidas preventivas en pro de mejorar siempre.

V. LA REPUTACIÓN ES UN ACTIVO PARA LAS ENTIDADES FINANCIERAS

Cuando una entidad financiera es vulnerada y perjudicada por ataques malintencionados, se puede ver afectado su capital, pero esto en ocasiones no es lo más importante, sino que pasa cuando sus clientes o proveedores se enteran de que hay fallas de seguridad y que les han robado información sin poder hacer nada, se pierde la reputación que puede llegar a ser un activo igual o más importante que los demás, recuperar la reputación puede ser muy difícil y puede llevar mucho tiempo para lograrlo.

Si los clientes o proveedores deciden cambiar de una entidad a otra, son libres de tomar las decisiones pertinentes y tener el dinero donde sientan el respaldo y confianza de expectativas para hacerlo, estos comportamientos a largo plazo pueden representar perdidas económicas incalculables, el cliente es libre de elegir la mejor opción.

La reputación de una organización puede desvanecerse en forma inmediata después de algún incidente de seguridad en el que se vea afectada la credibilidad de los clientes e inversionistas, este tipo de eventos a parte de la pérdida económica que puede llegar a causar, que vendría siendo algo menor o importante, como si lo es el tiempo que se

puede tardar una entidad bancaria en recuperar la reputación e imagen, que podrían ser meses o tal vez años.

Por este motivo en particular las organizaciones del sector financiero se ven obligadas a tomar medidas constantemente**,** e intentar adelantarse a los ataques que puedan ocasionar este tipo de impacto negativo, fortaleciendo la seguridad informática de la compañía, pero este trabajo sería imposible sin contar con profesionales de hacking ético que trabajan en pro de mejorar la seguridad constantemente y dificultar a los atacantes los ingresos no autorizados sobre la información sensible de las compañías, no solo del sector financiero sino de todas las organizaciones que puedan ser objetivo por los **hackers de sombrero negro.**

VI. ACTUALIDAD DEL HACKING ÉTICO

El hacking ético ha ido tomando fuerza, a medida que las empresas crecen y la dependencia tecnológica es mayor, se empieza hacer más común este término y escuchar de esta práctica es una realidad, se hace necesaria intentar poner freno a los ataques constantes por cibercriminales. El hacking ético se ha ido tomando su lugar en la seguridad general de las organizaciones.

A medida que los servicios tecnológicos crecen y las transacciones o compras online están en constante aumento, es notable que las personas cada vez más utilizan estos servicios que ofrecen los bancos para facilitar el tiempo que se puede invertir en este tipo de tareas, pero esto trae consigo una tendencia de aumento de incidentes de seguridad, así como aumento en ataques de phishing contra entidades bancarias, y así como se va mejorando cada día la seguridad en estas entidades, también mejoran la forma de atacar con herramientas sofisticadas y en mayor cantidad, queriendo siempre vulnerar la seguridad quebrantando contra la los pilares de la seguridad: **confidencialidad**, **integridad** y **disponibilidad** de la información. Existen varios mecanismos de engaño para que un programa de este tipo logre llegar a una red bancaria, todo viaja a través del internet facilitando este tipo de ataques, abriendo un correo de publicidad llamativa como ganarse una beca o un viaje, que haya un anuncio de un programa gratuito, hasta un link en una red social puede llegar a ocasionar un hueco de seguridad en una red organizacional. El hacking ético tiene como función verificar los niveles de seguridad actuales en el momento que se hace el análisis, se intenta descubrir **vulnerabilidades** y así mismo corregirlas antes de que un malhechor llegue a ellas y pueda explotarlas de manera perjudicial para la organización.

VII. TENDENCIA DE ATAQUES DE SEGURIDAD

El uso de internet va en aumento no solo desde pc sino dispositivos móviles que acceden a estos servicios de red. La seguridad informática se ha vuelto la mayor preocupación para los profesionales de la seguridad.

El Incremento de nuevos virus, troyanos, botnets, cada vez es más fácil crear este tipo de programas y en muchas ocasiones sin conocimientos técnicos previos, basta con utilizar una herramienta buscada en internet y generarlos sin que se pueda controlar, para luego ser mandados a la red, según PandaLabs el 70% de los troyanos analizados tienen como objetivo principal obtener los datos bancarios de las víctimas. Pero es un dato menor cuando todo cambia en un par de horas. Cada segundo se está creando un nuevo troyano, Algunos de estos virus son creados solo por diversión pero en casos más profundos se encuentra toda una economía de mercado criminal en la cual el costo beneficio para el hacker puede resultar tentador y beneficioso, aunque en muchas ocasiones también se hace por reto propio de poner a prueba los conocimientos y lograr vulnerar en sector financiero y robar las bases de datos con datos de números de tarjetas de crédito, nombre familiares, celular y demás datos sensibles que resulten graves no solo para la entidad financiera la cual debe garantizar que estos datos no sean vulnerados por personas inescrupulosas, sino para los clientes que pueden ser víctimas de robos o

cobros sin justificación. Esto es solo el inicio del impacto que puede generar un ataque con éxito. Se debe intentar ir un paso adelante cerrando las brechas de seguridad al máximo.

VIII. CONCLUSIONES

La seguridad es importante por lo que se deben tomar medidas preventivas, en la actualidad el **hacking ético** es una opción a mitigar el riesgo de ataque, estar en constante monitoreo y revisión con el fin de cerrar brechas de seguridad que puedan afectar el servicio.

Se debe estar en constante investigación con respecto a las **vulnerabilidades** que se haya en los sistemas, con el fin de que se puedan tomar las medidas respectivas a tiempo. Antes de que sean explotadas por un delincuente.

Tal vez nunca se podrá evitar que se genere software malicioso constantemente, pero lo que si debemos tener como procedimiento es hacer pruebas de **vulnerabilidad** periódicamente, de esta forma poder corregir las fallas de seguridad que se encuentren en su momento a tiempo y evitar el robo de información **confidencial**.

Los ataques online o electrónicos que se presentan en la actualidad no solo son más frecuentes sino más sofisticados lo que obliga a estar en constante actualización en temas de seguridad, y a estar probando constantemente la efectividad de controles, revisando fallas y corrigiendo.

El sector financiero es el objetivo favorito de los delincuentes, por lo que no se debe descuidar la seguridad en ningún momento, cualquier error se puede cobrar con la perdida de reputación de la entidad.

REFERENCIAS

[1]. Información de reporte ataques a entidades financieras. Disponible: http://www.geek.com.mx/2015/08/el-sector-financiero-recibe-300-mas-ataques-que-otras-industrias/

[2].Dato referencia estadístico sobre ataque a instituciones de servicios financieros. Disponible: http://www.oem.com.mx/elmexicano/notas/n3903479.htm

[3]. Definición del termino hacking ético. Disponible: http://revista.seguridad.unam.mx/numero-12/hacking-%C3%A9tico-mitos-y-realidades

[4]. Definición términos Hackers de sombrero blanco (White Hat Hackers) y Los hackers de sombrero negro (Black Hat Hackers) http://blog.capacityacademy.com/2012/07/11/7-tipos-de-hackers-y-sus-motivaciones/

[5]. Circular 042 del 2012 numeral 7”análisis de vulnerabilidades”. Disponible: https://www.superfinanciera.gov.co/SFCant/Normativa/NormasyReglamentaciones/cir007/cap12_seguridad_calidad.doc

[6] Definición norma ISO 27001. Disponible: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001

[7] Definición termino PCI DSS: https://es.wikipedia.org/wiki/PCI_DSS

[8]. Contenido ley 1328 del 2009. Disponible: www.nuevalegislacion.com/files/susc/cdj/conc/l_1328_09.doc